

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-108363

(43)Date of publication of application : 11.04.2003

(51)Int.Cl. G06F 7/58

G09C 1/00

H03K 3/84

(21)Application number : 2001-294835 (71)Applicant : TOSHIBA CORP

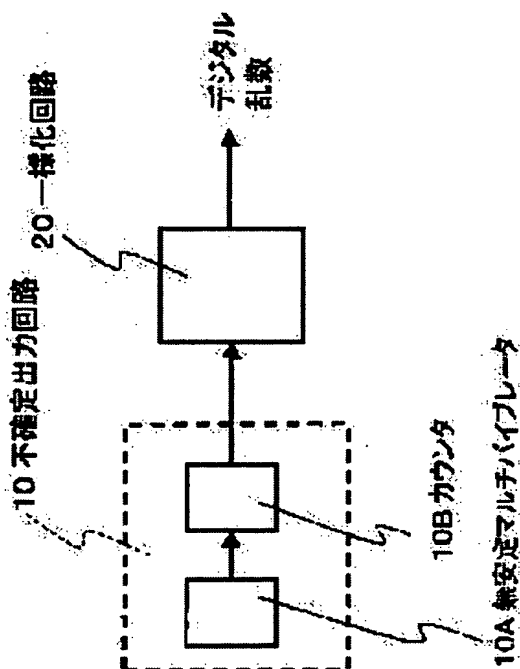
(22)Date of filing : 26.09.2001 (72)Inventor : FUJITA SHINOBU

UCHIDA KEN

KOGA JUNJI

OBA RYUJI

(54) RANDOM NUMBER GENERATION CIRCUIT



(57)Abstract:

PROBLEM TO BE SOLVED: To provide a random number generation circuit that generates random numbers of high genuineness and permits to convert it into a small integrated circuit.

SOLUTION: In an astable vibrator (10A), such an element is introduced that circuit element characteristic determining the vibration period thereof tends to fluctuate temporally based on a physical phenomenon, and the vibration period of the vibrator is made to fluctuate temporally and irregularly. By reading the vibrator signal fluctuating irregularly with a counter on a fixed

clock, it becomes possible to acquire a random digital signal train of 0 and 1.

4

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-108363

(P2003-108363A)

(43) 公開日 平成15年4月11日 (2003.4.11)

(51) Int.Cl. ⁷	識別記号	F I	テマコード* (参考)
G 0 6 F 7/58		G 0 6 F 7/58	A 5 J 0 4 9
G 0 9 C 1/00	6 5 0	G 0 9 C 1/00	6 5 0 B 5 J 1 0 4
H 0 3 K 3/84		H 0 3 K 3/84	Z

審査請求 未請求 請求項の数 7 O L (全 9 頁)

(21) 出願番号 特願2001-294835 (P2001-294835)

(22) 出願日 平成13年9月26日 (2001.9.26)

(71) 出願人 000003078

株式会社東芝

東京都港区芝浦一丁目1番1号

(72) 発明者 藤田 忍

神奈川県川崎市幸区小向東芝町1番地 株

式会社東芝研究開発センター内

(72) 発明者 内田 建

神奈川県横浜市磯子区新杉田町8番地 株

式会社東芝横浜事業所内

(74) 代理人 100088487

弁理士 松山 允之 (外1名)

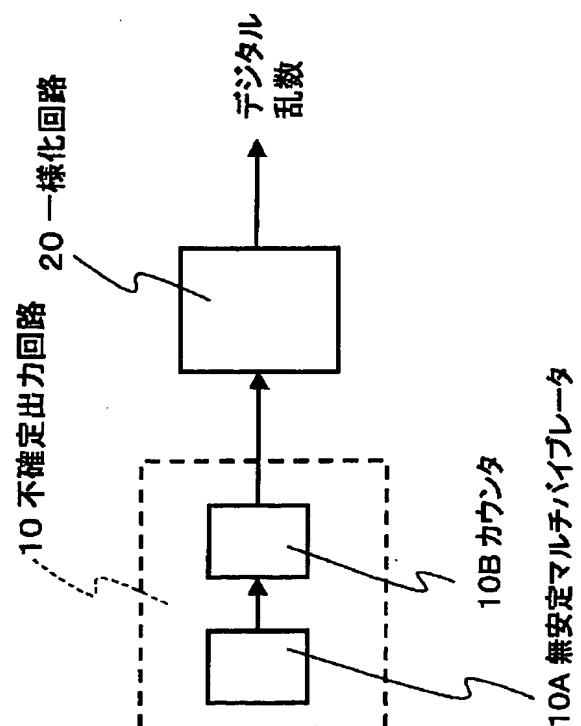
最終頁に続く

(54) 【発明の名称】 乱数生成回路

(57) 【要約】

【課題】 真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することを目的とする。

【解決手段】 無安定バイブレータ (10A) に、その振動周期を決定する回路要素特性が、物理現象に基づいて時間的に揺らぎやすいような素子が導入されており、バイブレータの振動周期が時間的に不規則に変動するようにされている。このように不規則に揺らいでいるバイブレータ信号をカウンタが一定のクロックで読み出すことにより、「0」と「1」のランダムなデジタル信号列を得ることができる。



【特許請求の範囲】

【請求項1】不確定なデジタル信号列を生成する不確定出力回路を備え、

前記不確定出力回路は、「0」レベルと「1」レベルとを交互に出力し、前記「0」レベルと前記「1」レベルをそれぞれ保持する時間を決定する回路要素のうちの少なくともいずれかの特性が時間とともに変動することにより、前記「0」レベルと前記「1」レベルを保持する時間のいずれかが変動するマルチバイブレータを有することを特徴とする乱数生成回路。

【請求項2】前記不確定出力回路は、前記マルチバイブレータから出力される前記「0」レベルと前記「1」レベルとの信号列を一定の周期で読み取るカウンタをさらに有することを特徴とする請求項1記載の乱数生成回路。

【請求項3】前記カウンタが読み取る前記一定の周期は、前記マルチバイブレータから出力される前記「0」レベルと前記「1」レベルとの信号列における平均的な遷移の周期よりも十分に長いことを特徴とする請求項2記載の乱数生成回路。

【請求項4】前記変動する前記回路要素の特性は、MOSトランジスタのチャネル抵抗であることを特徴とする請求項1～3のいずれか1つに記載の乱数生成回路。

【請求項5】前記不確定出力回路から出力される前記不確定なデジタル信号列における「0」と「1」の出現頻度をカウントするカウント回路と、前記カウント回路によりカウントした前記出現頻度に基づいたフィードバック信号を前記マルチバイブレータの前記回路要素に与えるフィードバック回路と、をさらに備えたことを特徴とする請求項1～4のいずれか1つに記載の乱数生成回路。

【請求項6】前記不確定出力回路から出力された前記不確定なデジタル信号列に含まれる複数のデジタル信号の排他的論理和を演算しその演算結果を乱数として出力する論理演算回路をさらに備えたことを特徴とする請求項1～5のいずれか1つに記載の乱数生成回路。

【請求項7】「0」と「1」との出現頻度が1:1であるデジタル信号列と、前記不確定出力回路から出力される前記不確定なデジタル信号列と、の排他的論理和を演算しその演算結果をデジタル乱数列として出力する論理演算回路をさらに備えたことを特徴とする請求項1～5のいずれか1つに記載の乱数生成回路。

【発明の詳細な説明】**【0001】**

【発明の属する技術分野】本発明は、乱数生成回路に関し、特に、デジタル論理回路によりコンパクトに構成することが可能でしかも真性度が高い乱数を発生し、暗号アルゴリズムに用いても好適な乱数生成回路に関する。

【0002】

【従来の技術】デジタル乱数は、確率過程を伴う現象の

シミュレーションや、セキュリティーに用いる暗号アルゴリズムでの暗号鍵の生成などに用いられる。従来、デジタル乱数としては、CPUで計算によって作られる「擬似乱数」が用いられてきた。この擬似乱数は、典型的には、「フィードバックシフトレジスタ」と呼ばれる論理回路で作られる。

【0003】これに対して、抵抗やダイオードに発生する雑音を使って乱数を作り出す方式も実用化されている。この場合、乱数に偏りや周期性などは見られなくなり、「真性乱数」に近いものが得られる。このタイプの乱数生成回路においては、雑音源の素子に一定電流を流して発生する雑音をハイパスフィルター回路に通して、AC成分を取り出し、それをアナログ回路で増幅したのち、AD変換してデジタル化する。このとき、ある値を閾値として、それを越えるものを「1」、それ以下のものを「0」というようにする。さらに、出てきた乱数列は偏りが出るため、それをデジタル回路で補正してから用いる場合が多い。

【0004】

【発明が解決しようとする課題】CPUで作る擬似乱数は、初めに与えた数字（種）が同じであれば、同じ乱数を発生させてしまうことや、レジスタの個数に基づく周期性をもってしまうため、乱数としては適当でないことが知られている。特に、セキュリティーに用いる場合には、「暗号鍵」を破られる危険性を産む原因となる。

【0005】一方、雑音を増幅するタイプだと、一般的に抵抗やダイオードの熱雑音やショット雑音はアナログ信号であり、また出力が小さいために、アナログ増幅回路の構成が大規模となり、集積化、小型化が困難である。特に、暗号セキュリティー機能を搭載したICカード等の小型機器に組み込むことは困難である。

【0006】つまり、周期性を持たない質の高い乱数を発生させ、かつ小型の集積回路が必要とされつつある。

【0007】小型化のためには、TTLやCMOS等のデジタル回路で構成することが望ましい。しかし、デジタル回路は、基本的にある入力に対して同一の出力を与えるので、アルゴリズム的な処理で乱数を作ることしかできない。このため、フィードバックシフトレジスタと同様に擬似乱数しか作り出せない。

【0008】この矛盾を解決するためには、デジタル回路で、出力が不確定になる回路を作る必要がある。

【0009】本発明は、かかる課題の認識に基づいてなされたものである。すなわち、その目的は、真性度の高い乱数を発生させ、かつ小型の集積回路化が可能な乱数生成回路を提供することにある。

【課題を解決するための手段】上記目的を達成するため、本発明の乱数生成回路は、不確定なデジタル信号列を生成する不確定出力回路を備え、前記不確定出力回路は、「0」レベルと「1」レベルとを交互に出力し、前記「0」レベルと前記「1」レベルをそれぞれ保持する

時間を決定する回路要素のうちの少なくともいずれかの特性が時間とともに変動することにより、前記「0」レベルと前記「1」レベルを保持する時間のいずれかが変動するマルチバイブレータを有することを特徴とする。

【0010】上記構成によれば、マルチバイブレータを構成する素子の特性の変動に応じた不確定な信号列が得られ、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。

【0011】ここで、前記不確定出力回路は、前記マルチバイブレータから出力される前記「0」レベルと前記「1」レベルとの信号列を一定の周期で読み取るカウンタをさらに有するものとすれば、マルチバイブレータからの信号列から不確定なデジタル信号列を得ることができる。

【0012】また、前記カウンタが読み取る前記一定の周期は、前記マルチバイブレータから出力される前記「0」レベルと前記「1」レベルとの信号列における平均的な遷移の周期よりも十分に長いものとすれば、マルチバイブレータから出力される信号列の周期性の影響を排除することができる。

【0013】また、前記変動する前記回路要素の特性は、MOSトランジスタのチャネル抵抗であるものとすれば、ゲート絶縁膜にトラップを形成することにより、マルチバイブレータからの出力を不確定なものとすることができる。

【0014】また、前記不確定出力回路から出力される前記不確定なデジタル信号列における「0」と「1」の出現頻度をカウントするカウント回路と、前記カウント回路によりカウントした前記出現頻度に基づいたフィードバック信号を前記マルチバイブレータの前記回路要素に与えるフィードバック回路と、をさらに備えたものとすれば、不確定出力回路からのデジタル出力列における「偏り」を抑制することができる。

【0015】また、前記不確定出力回路から出力された前記不確定なデジタル信号列に含まれる複数のデジタル信号の排他的論理和を演算しその演算結果を乱数として出力する論理演算回路をさらに備えたものとすれば、「偏り」のない乱数が得られる。

【0016】または、「0」と「1」の出現頻度が1:1であるデジタル信号列と、前記不確定出力回路から出力される前記不確定なデジタル信号列と、の排他的論理和を演算しその演算結果をデジタル乱数列として出力する論理演算回路をさらに備えたものとすれば、「偏り」のない乱数列が得られる。

【0017】

【発明の実施の形態】以下、図面を参照しつつ、本発明の実施の形態について詳細に説明する。

【0018】図1は、本発明の乱数生成回路の要部構成を表すブロック図である。

【0019】すなわち、本発明の乱数生成回路は、不確

定出力回路10と、その出力を受け一様化回路20とを備える。

【0020】不確定出力回路10は、デジタル回路で構成した無安定マルチバイブレータ10Aとカウンタ10Bとを有する。無安定マルチバイブレータ10Aは、その振動周期を決定する抵抗の抵抗値あるいはコンデンサの容量が、物理現象に基づいて時間的に揺らぎやすいような素子が導入されており、マルチバイブレータの振動周期が時間的に不規則に変動するようにされている。

【0021】そして、このように不規則に揺らいでいるバイブレータ信号をカウンタ10Bが一定のクロックで読み出すことにより、「0」と「1」のランダムなデジタル信号列を得ることができる。

【0022】この方法で得られた「0」と「1」とのデジタル信号列の配列は、マルチバイブレータを構成する素子の特性に依存しているので、「0」と「1」の出現頻度に「偏り」が生ずる場合がある。

【0023】そこで、このような場合には、一様化回路20において、それらを再度デジタル処理して、偏りを無くして真性度の高いデジタル乱数を得る。

【0024】このようにすれば、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。

「0」と「1」の頻度を補正する回路も、比較的小規模な論理回路で構成可能である。

【0025】また、本発明においては、一様化回路20は必須ではなく、不確定出力回路10から出力されるデジタル乱数列が十分に一樣であるような場合には、一様化回路20を設ける必要はない。

【0026】以下、本発明の不確定出力回路10において用いる無安定マルチバイブレータについて説明する。

【0027】図2は、通常「無安定マルチバイブレータ」と呼ばれるデジタル回路を表す模式図である。この無安定マルチバイブレータは、フリップフロップ型に接続された2つのNAND回路11、12に、抵抗R1、R2とコンデンサC1、C2とがそれぞれ接続された構成を有する。

【0028】このマルチバイブレータは、B側のコントロール入力をONすると、動作が開始する。すなわち、始めにB側のコントロール入力が「0」である（すなわち、コンデンサC2が空）とすると、NAND回路12の出力が「1」になり、A側にあるコンデンサC1を充電し始める。あるところまで充電が進むと、A側の入力が「0」となるので、A側のNAND回路11の出力は「1」となり、今度はB側のコンデンサC2を充電し始める。これが交互に繰り返されるので、A側のNAND回路11の出力は、「1」と「0」とを交互に繰り返したものとなる。

【0029】この繰り返しの周期は、コンデンサC1、C2の充電時間で決まり、コンデンサの容量と抵抗R1、R2の大きさの積、すなわち(C×R)に比例す

る。

【0030】図2に表したマルチバイブレータの場合、繰り返しの周期は およそ $0.7(C1R1+C2R2)$ となる。

【0031】本発明においては、この繰り返し周期が変動するように独特の素子を配置する。

【0032】図3は、本発明の乱数発生回路において用いるマルチバイブレータの要部構造を例示する模式図である。

【0033】すなわち、同図に表した無安定マルチバイブレータは、抵抗 $R1$ 、 $R2$ の少なくともいずれかを、チャネル抵抗が時間的な揺らぎを持つ特殊なMOSトランジスタ14に置換した構造を有する。

【0034】図4は、MOSトランジスタ14の要部構造を例示する概念図である。

【0035】このMOSトランジスタのゲート絶縁膜14Gには、複数の電子トラップTが形成されている。チャネル14C中を通過する電子は、絶縁膜14Gをトンネルして頻繁にトラップTに捕獲され、また捕獲されている電子がチャネル14Cにトンネルできるように、素子パラメータが調節されている。

【0036】電子トラップTは、例えば、シリコン酸化膜の絶縁膜中にシリコンのナノクリスタルを分散させたり、電子トラップの多い $SiON_x$ （窒化酸化シリコン）を絶縁膜14Gとして用いたりすることで形成することができる。

【0037】または、絶縁膜14Gの形成の途中で中断し、異なるガス雰囲気などに晒すことにより、欠陥や不純物を導入することによっても、電子トラップTを絶縁膜14Gの中に形成することが可能である。

【0038】トラップTに電子がトラップされると、クーロン相互作用によって、絶縁膜14Gとの界面付近のチャネル14Cを移動する電子が散乱を受け、チャネル抵抗が上昇する。

【0039】従って、このMOSトランジスタ14の設計にあたっては、チャネル14Cを薄く絞ることにより、電子トラップTへの電子の捕獲と脱離によって、MOSトランジスタのチャネル抵抗が、その平均値に対して数十%程度揺らぐように、初期ゲート電圧を調整しておくことが望ましい。また、ゲート幅（チャネル幅）が狭いほど、チャネル抵抗の変動率が大きくなるので、ゲート幅の狭いMOSFETが望ましい。

【0040】マルチバイブレータの周期は、コンデンサ $C1$ 、 $C2$ の容量とMOSトランジスタ14のチャネル抵抗で（より厳密には、トランジスタ14の寄生容量も影響する）決まるので、トランジスタのチャネル抵抗が数十%揺らぐと、マルチバイブレータの周期も数十%揺らぐ。

【0041】図5は、トランジスタのチャネル抵抗が時間的に揺らいでいる状態を表す模式図である。この「揺

らぎ」の頻度あるいはピッチは、当然のことながら一定ではなく、またその振幅も一定ではない。「揺らぎ」の発生頻度は、トラップTへの電子の捕獲頻度と、トラップTにおける電子の滞在時間に依存する。従って、「揺らぎ」の発生頻度が最適な範囲となるように、トラップTの種類やその形成条件を調節することができる。

【0042】MOSFET以外にも、フォトトランジスタやフォトダイオードを使うことも出来る。図11にPIN型フォトダイオードを使う例を示す。フォトダイオード21は微弱な光を感知して、光電流に変換する素子である。その原理に基づき、光があたるとその光量によって抵抗が著しく変化する。そこで、フォトダイオードの近くに小型のLED型の発光素子22を設置しておき、マルチバイブレータ回路を動かすための制御電圧で発光素子が動作するようにしておく。発光素子の光量は、ノイズなどにより変動するので、その変動にตอบสนองしてフォトダイオードは抵抗成分を変化させるので、マルチバイブレータの周期もそれにつれて変動する。発光素子22の光量は微弱で良いので、サブ μm サイズのゲートを有するMOSFETのドレインに高電界を加えてホットエレクトロンを生じさせ、それが緩和する過程での発光を使っても良い。

【0043】さて、本発明においては、このように「揺らぎ」が生ずるトランジスタ14を設けることにより、無安定マルチバイブレータの動作を不安定化させる。

【0044】図6は、本発明における無安定マルチバイブレータから得られる出力信号を例示する概念図である。このように一定周期でないデジタル信号の変化を、この変化の周期よりも十分長い周期のカウンタ10Bで読み取ると、その値は1ビットの乱数列となる。

【0045】ここで、カウンタ10Bの読み取り周期をマルチバイブレータ10Aの出力信号の変化の周期よりも十分に長くするのは、得られる乱数列に周期性が生ずるのを防ぐためである。周期性を十分に低下させるためには、マルチバイブレータ10Aの出力信号の変化の周期に対して、カウンタ10Bの読み取りの周期を10倍あるいはそれ以上とすることが望ましい。

【0046】このようにして得られたデジタル乱数列が十分に一樣であるような場合には、これをそのまま、乱数列として利用することができる。

【0047】一方、このようにして得られた乱数列の「0」と「1」の出現確率に「偏り」が見られる場合には、一樣化回路20において、「偏り」を補正する。

【0048】そこで、次に、一樣化回路20について説明する。

【0049】図7は、本実施例における一樣化回路の動作を説明するための概念図である。

【0050】同図に表したように、不確定出力回路10の出力を時系列的に、 Q_n, \dots, Q_{n+k} として、これらの $k+1$ 個のデータにXOR（排他的論理和）の論理演

算を施す。その結果をTとする。不確定出力回路1の出力において、「1」の出現確率をp、「0」の出現確率を $1-p$ とすると、Tが1となる確率は、 $0.5 + 0.5 \cdot (1 - 2p)^{k+1}$ となる。kが大きくなるほど、確率が0.5に近づき、偏りが補正される。

【0051】前述した第1実施例において実際に試作したSR-FFでは、「偏り」が大きくほぼ $p=0.1$ であった。k=10の場合、Tが1となる確率は0.543となり、K=20の場合、0.505、K=30の場合、0.5005と0.5に近づき、ほとんど「偏り」がなくなる。

【0052】kが大きくなると、乱数の生成速度が遅くなってしまうが、例えば電源をON、OFFする周期を30MHzにすると、 $k=30$ としても約1Mbit/秒の速度でデジタル乱数列を生成することができるので、実用上は問題とならない場合が多い。

【0053】また、このようにして得られた乱数列データをフィードバックシフトレジスタのシード(種)に使っても良い。

【0054】また、以下に説明するような方法を用いれば、簡便に「0」と「1」の出現確率を均等にすることができる。

【0055】すなわち、デジタル信号Pが「1」になる確率をp、デジタル信号Qが「1」になる確率をqとすると、PとQとの排他的論理和(XOR)の演算値Tが「1」となる確率と、「0」となる確率の差は、次式により表される。

$$4(0.5-p)(0.5-q) \cdots (1)$$

従って、「Pが「1」になる確率が0.5」であれば、Qが「1」になる確率が $1/2$ でなくても、PとQとの排他的論理和の演算値Tの「0」と「1」の出現確率は等しくなる。

【0056】ここで、図10に表したように、カウンタ10Bへの入力信号を分岐してT型のフリップフロップ20Bに入れると、周期が2倍の信号になり、これは不確定出力回路10の出力と同じタイミングで「0」と「1」とが交互に並ぶ信号となる。この信号は、当然に「0」と「1」の出現率が等しい。従って、この信号と不確定出力回路10の信号との排他的論理和をとると、その演算出力Tにおいては当然に「0」と「1」の出現確率が等しく、真性度の高いデジタル乱数列として用いることができる。

【0057】また、図11に表したように、フィードバックシフトレジスタ(FSR)20Cにより、カウンタ10Bと同じクロックで作った擬似乱数Rは、「0」と「1」とを均等に出力するので、これと不確定出力回路10の出力との排他的論理和をとると、その演算値Tは「0」と「1」の出現率が等しく、真性度の高いデジタル乱数列として用いることができる。

【0058】一方、本発明においては、不確定出力回路

10の出力をモニタしフィードバックをかけることによって「偏り」を補正することができる。

【0059】図10は、このような乱数生成回路の要部構成を表す模式図である。

【0060】本具体例においては、無安定マルチバイブレータのトランジスタ14のゲート14Gに、一様化回路20がフィードバックを加える。このようなフィードバックにより、不確定フリップフロップの「0」と「1」の出現確率を均等に近くすることができる。

【0061】すなわち、同図において、不確定出力回路10の出力をデジタルカウンタ20Dでカウントしておき、「0」と「1」のカウントの差分に応じて、フィードバック回路20Eが所定のゲート電圧をマルチバイブレータのMOSトランジスタのゲート14Gに印加する。

【0062】すると、MOSトランジスタ14のチャネル抵抗の相対的な揺らぎの大きさが調節され、「偏り」を修正することが可能である。

【0063】この場合にも、図7乃至図9に関して前述したように、「偏り」をなくす論理回路を組み合わせると、乱数の「偏り」をさらに小さくできる。この場合、前述したXORをとるデータkの数が少なく済むので、乱数の生成速度を上げることができる。

【0064】以上、具体例を例示しつつ本発明の実施の形態について説明した。しかし、本発明は、上述した各具体例に限定されるものではない。

【0065】例えば、本発明において用いる不確定出力回路および一様化回路の具体的な構成に関しては、上記の具体例に限定されず、その機能あるいは作用が同様な全ての回路に置換したのもも本発明の範囲に含まれる。

【0066】また、上述した具体例においては、マルチバイブレータ10Aの一方のNAND回路だけにMOSトランジスタを配置した場合を例示したが、A側とB側の両方に設けても良い。

【0067】また、マルチバイブレータの容量C1、C2のいずれかが時間的に変動するようにしてもよい。

【0068】また、本発明においては、無安定マルチバイブレータに限らず、「単安定マルチバイブレータ」や「双安定マルチバイブレータ」を用いても同様の不安定な出力を形成させることができ、これらも本発明の範囲に含まれる。

【0069】さらに、前述した複数の実施例のうち、不確定出力のデジタル回路と、デジタル出力の頻度を補正する回路とを部分的に組み合わせたものも、乱数生成回路として使用可能であり、本発明の範囲に含まれる。

【0070】また、本発明の乱数生成回路によって作られたデジタル乱数は、そのまま使用することもできるが、フィードバックシフトレジスタの種として用いることにより、新たな乱数を生成することもできる。

【0071】

【発明の効果】以上詳述したように、本発明によれば、無安定マルチバイブレータにおいて、その出力を不安定とする素子を導入することにより、乱数生成回路を少ない論理ゲート数で構成できるので、小規模な回路で済む。

【0072】また同時に、「0」と「1」の頻度を補正する一様化回路も、比較的小規模な論理回路で構成可能である。

【0073】そして、乱数の元になる現象は、無安定マルチバイブレータ10Aを構成する素子の物理現象に基づくものであるため、同一の入力に対して、不確定の出力が得られるため、乱数列に周期性が出ず、乱数を推定可能な疑似乱数とは異なる質の高い乱数を得ることができる。

【0074】すなわち、本発明によれば、真性度が高い乱数をコンパクト且つ低価格で実現できるようになり、例えばICカードなどに応用してセキュリティの確実な安価なカードシステムを実現できる点で産業上のメリットは多大である。

【図面の簡単な説明】

【図1】本発明の乱数生成回路の要部構成を表すブロック図である。

【図2】通常「無安定マルチバイブレータ」と呼ばれるデジタル回路を表す模式図である。

【図3】本発明の乱数発生回路において用いるマルチバイブレータの要部構造を表す模式図である。

【図4】MOSトランジスタ14の要部構造を例示する概念図である。

【図5】トランジスタのチャネル抵抗が時間的に揺らい

でいる状態を表す模式図である。

【図6】本発明における無安定マルチバイブレータから得られる出力信号を例示する概念図である。

【図7】本発明における一様化回路の動作を説明するための概念図である。

【図8】一様化回路のもうひとつの具体例を表す模式図である。

【図9】一様化回路のもうひとつの具体例を表す模式図である。

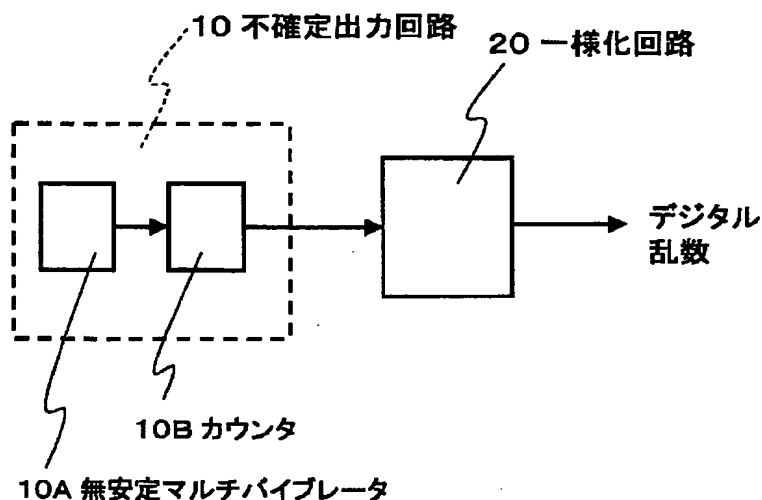
【図10】本発明の具体例の乱数生成回路の要部構成を表す模式図である。

【図11】フォトダイオードを用いたマルチバイブレータを表す模式図である。

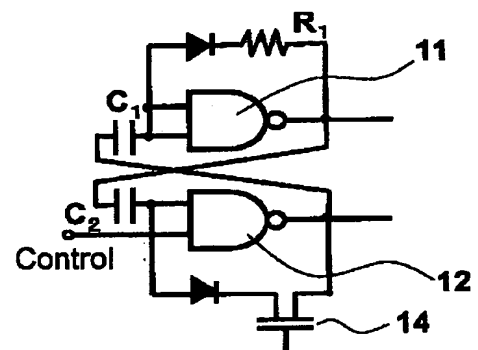
【符号の説明】

- 10 不確定出力回路
- 10A 無安定マルチバイブレータ
- 10B カウンタ
- 11、12 NAND回路
- 14 トランジスタ
- 12C チャンネル
- 12G ゲート絶縁膜
- 20 一様化回路
- 20A XOR回路
- 20B フリップフロップ
- 20C FSR
- 20D デジタルカウンタ
- 20E フィードバック回路
- T トラップ
- 21 フォトダイオード
- 22 発光素子

【図1】



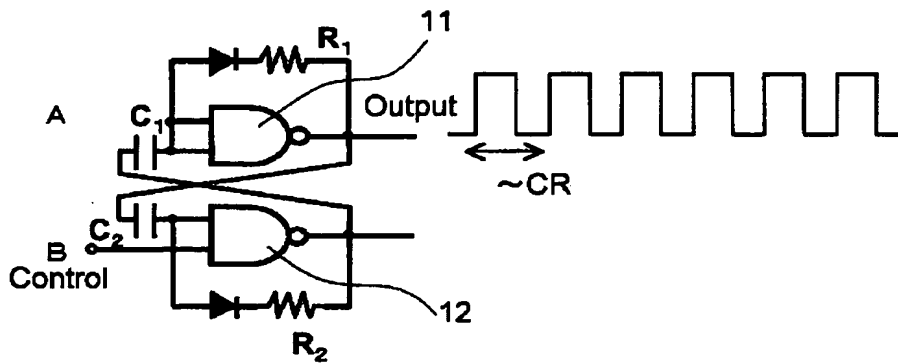
【図3】



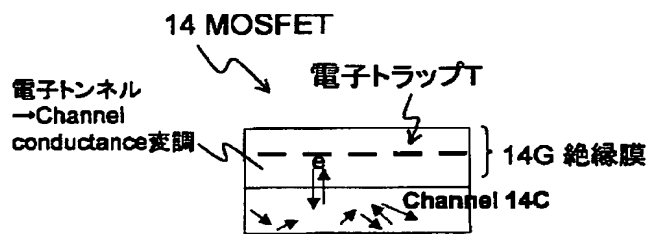
【図5】



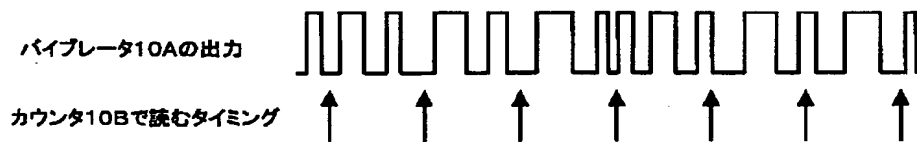
【図2】



【図4】



【図6】



【図7】

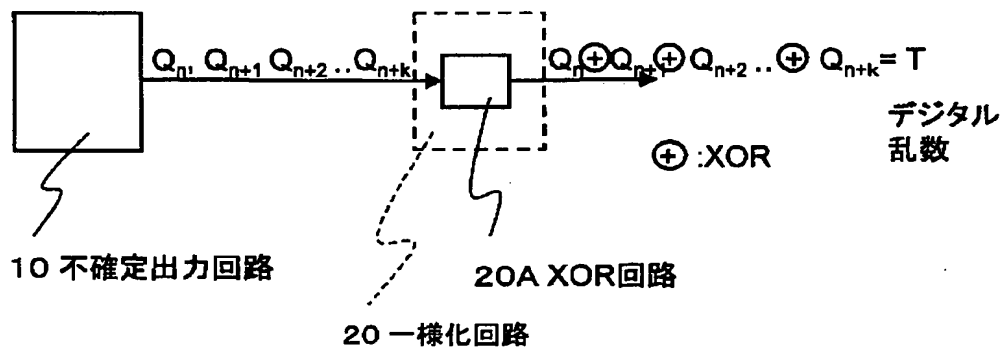
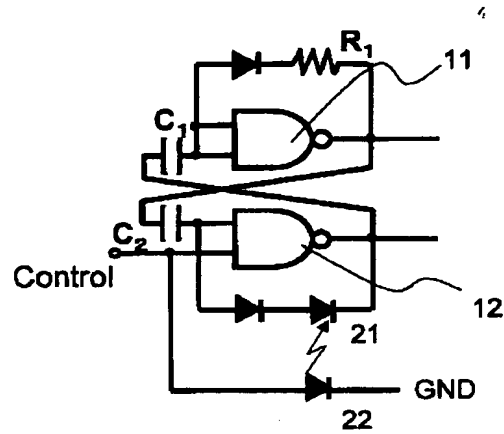


Figure 1 is a block diagram of a digital random number generator. It consists of three main components: a shift register (10), a T-Flip Flop (20B), and an XOR circuit (20A). A clock signal (CLK) is provided to both the shift register (10) and the T-Flip Flop (20B). The shift register (10) outputs a sequence of bits $Q_n, Q_{n+1}, Q_{n+2}, \dots, Q_{n+k}$. The T-Flip Flop (20B) outputs a sequence of bits 0, 1, 0, 1, ... These two sequences are fed into the XOR circuit (20A), which produces the digital random numbers $T_n, T_{n+1}, T_{n+2}, \dots, T_{n+k}$.

【図11】



フロントページの続き

(72)発明者 古賀 淳二
神奈川県横浜市磯子区新杉田町8番地 株
式会社東芝横浜事業所内

(72)発明者 大場 竜二
神奈川県横浜市磯子区新杉田町8番地 株
式会社東芝横浜事業所内

Fターム(参考) 5J049 AA01 AA17 CA03 CA10
5J104 FA10

TO:中嶋__規夫
CC:宮本__光秀
主題：A特許管理番号
送信者：河野__亨
受信日：06/08/04 14:38
属性：指定なし
添付ファイル：なし
中嶋 様 cc(宮本)

お世話になっております。

OLED関係の特許について、予備検討会を行いたいと考えております。お願いできますでしょうか？

「OLED素子の低電力焼付きおよび温度補正システム」・・・UR0639
お忙しい中申し訳ありませんが、宜しくお願いします。

UR/606 河野